Due 3 30 July

NFIB

DEPUTY DIRECTOR
DOD COMPUTER SECURITY CENTER

15 July 1982

SUSPENSE: 2 Aug 82

C11
C111

IN TURN

1. Attached is a draft of some material being considered by the CIA/ISSG as part of their review of DCID 1/16 revisions. This may be of particular interest in your look at tying environments to our evaluation criteria.

STAT

2. I will be having lunch with [redacted] (ISSG) on 3 Aug 82, so would appreciate any comments or suggestions you might have before then, in case this comes up.

[redacted]

STAT

cc: C13 (w/attach)

C1-115

'expose' vice 'endanger'

p2 "RESPONSIBILITIES",a.
Why is this paragraph in the document?

(DCIREG xx-x) Chapter II I.1
Reword the last sentence to make clearer that ISSO reports deficiencies to the NFIB member, etc.

I.3
Use "ADP secure system criteria required to meet the minimum standard... or secure criteria available... " vice present sentence.

I4
Why focus on WP alone? Why not digital PBX?, Voice Store and Forward? This section focuses on a single dedicated computer use. How about computer controlled copiers, other kinds of dedicated computer use? (I note especially that there is little or no reference to communications processors).

I.6 (line 6)
"...selected when_new_purchases_are_made"

II (re: levels of operation)
The level definitions, as written mix up two concepts; single vs. multiple security levels (and/or SCI designations) and whether processing is done for one or more organizations (NFIB members), a need-to-know issue. As the level definitions are written, Level I, only, is a single level, dedicated system. Levels II-V are various instances of (security) multi-levels (according to definitions established in the computer security community). Levels IV and V have agency/contractor specific requirements for need to know in addition to the security required.

As a first cut, the list of levels could be collapsed into 3 levels; present level I, a level II that is multisecurity/SCI levels for 1 NFIB member, and a level III that is multiple security/SCI levels for 2 or more NFIB members. Levels based on the number of NFIB members involved is not terribly useful when it comes to establishing the computer security standard/criteria for each level unless it is claimed that there is less threat/risk from (or in) a single NFIB member environment than one which has two or more NFIB members.

[As one of several asides, where is it strongly stated that need-to-know is strongly applied between projects, etc.? See section II.3.e]

The repetition of the phrase "Processing in this level may include unclassified program related applications software ...etc", does not make any sense. Why is it there? If the system is approved for processing classified collateral/SCI, why isnt it

approved for the development of program-related software up to is approved.

II.2

I would replace this with a simple statement that: the Principal Approving Authority only can accredit an ADP system serving 2 or more NFIB members. The Approval Authority or his designee can approve all others.

II.3

The inclusion of the level references is unnecessary.

II.3.b

The underlined part implies that one and only one SCI project may use a given terminal. Are there not instances where two or more SCI programs use a single terminal?

II.4 through II.6

Strongly urge rewrite of these sections entirely to:

1. Make reference to the DODCSC Computer Security Evaluation Criteria which defines 7 levels of systems to which basic computer security principles have been applied to produce a continuum of increasingly strengthened computer systems for processing classified information. [You could crib the introduction part of the criteria paper which motivates the principles, or do a cut-down rewrite of that part then incorporate the detailed description by reference.

2. Map (i.e. establish the linkage) between the criteria (levels) and the processing environments which the 5 levels in the DCIREG xx are addressing (or the reduced version which I attempted).

[As an aside, what you really need is an attempt to codify threat / risk environments. For example, in the Level I environment, in there is no threat (all users cleared/access approved to the material) and no risk (of accidental disclosure) for the same reason.

In the several cases of 2 or more SCI projects (where all people are assumed to be cleared to TOP SECRET) there exists no threat per se, but there is a risk of accidental disclosure. The risk seems to me to be the same regardless of whether the environment involves one NFIB member or more than one NFIB member.

In the cases where one or more SCI groups and only TS collateral are involved, it is again no threat, but a risk is involved. It is not clear to me that the risk is greater if some users are not SCI approved, but all users are TS cleared.

There is then the case where one or more SCI groups and one or more collateral security levels are involved. This case, regardless of how many NFIB members share the environment represents both a threat (due to the unevenness of the clearances) and a risk (of greater consequences of loss due to the uneven clearances) [Remember, the risk being talked of here is that of accidental disclosure and its possible consequences].

For each of the threat/risk environments (represented by the clearances and access approvals involved), you need to establish a minimum computer security standard such as those used in the DODCSC paper.

As an example, for the Level I environment of the DCIREG paper, a class C1 or C2 system (from the DODCSC paper) could easily suffice.

Because you can do no more at the present, you are attempting to upgrade contractor sites to class B1 systems (roughly). If you have only an all SCI environment (i.e. one or more SCI groups), a class C2 or B1 might suffice. If you have an SCI/TS collateral (only) environment, you might require a minimum class B1.

After you have made an initial mapping from your threat/risk environment, you may want to modify it on the basis of the users functionality. If the users are programming the system, there is an increased threat and risk. The increased threat comes about from the opportunity given for a user to act against a system. The increased risk comes about from the fact that program errors can cause systems to expose data by accident.

If users are merely transaction users (e.g. data retrieval, or supplying parameters to a program), there is a reduced threat and risk due to the limited actions a user can take, and the (often ad hoc) mediation on data performed by the application. I argue that the risk is reduced as well, but I am clearly on less firm ground for that assertion.

Thus, if a system with a given threat/risk profile (based on clearances and access approvals) requires a DODCSC computer system class L, provides general programming support for some or all of the users, you might require it to meet a computer security standard of class L+1. If the use is transaction only, you might require it to meet only class L-1 standards.

I think that this way of looking at the levels and the security standards that are appropriate illuminates the significant issues of what kind of security measures are appropriate to what kind of threat/risk environment, with substantially less opportunity for interpretive error. END OF ASIDE].

In the attached appendix, I have sketched how I would approach both the levels and the mapping to the DODCSC classes.

II.7

If the DCIREG will require all printed output from computer systems to carry the correct classification/SCI markings, then this section should include a requirement that all logical storage containers (files, data sets, program libraries, etc.) appropriate to the system will carry an internal security label. This is needed for access control anyway.

II.7.e.3

The paragraph is ambigious. If the sanitization of magnetic media is good enough to release the media, then let it go. Otherwise, dont let it go ever! If the problem of sensitivity comes in, either dont ever let media with SCI on it go, or do it on the basis of classification; TS and SCI-- Never. Secret and below, whenever. It is a very confusing paragraph.

II.8

Here is a place to say that all system output will be labeled. If such labeling is required, then there is no reason to prohibit remote printers located in appropriately secure spaces. If the labeling problem is wrapped up in having to enter output into an accountability system, then permit some form of "working paper" designation that has to be destroyed or entered into a accountability system in 30 days or so. From what I see, the (hidden) true reason for not labeling out put is the onorous burden of having to enter it and handle it in the framework of an accountabiliy system. I would personally rather have data labeled properly, even if it is outside of a formal accountability system . It seems there is much less opportunity to mishandle it if it is properly marked. There is an old security axiom "If it gets in the way, it wont get done!".

II.9

UNDER NO CONCEIVABLE CIRCUMSTANCES SHOULD REMOTE DIAGNOSTIC LINKS BE PERMITTED!!!

II.9.b

"knowledgable" of what?

I would prohibit the removal of magnetic media ; floppys, tapes, discs, etc. by maintenance personnel. If such media are needed for maintenance or diagnostic purposes, then let the maintenance personnel bring in a set to be left at the site. This should be spelled out in the DCIREG.

II.10

This section could use strengthing. If no one has any better words, you can look at the MITRE paper paper of 5/25/82 by John White (see Pat Alison) page 7. There are other audit tools available, lets get them used.

We can categorize computer threat/risk environments based on the number of SCI categories and the type of classification(s) found on a given system. Figure 1 distinguishes 5 threat/risk environments as a function of these two variables.

Number of SCI Categories	Collateral Security Levels: None	TS Only	TS & below (mixed)
None	Type A	Type B	Type D
1	Type B	Type C	Type E
>1	Type C	Type C	Type E

Figure 1

Threat/Risk Types as a Function of the Number of SCI Categories and Collateral Security Levels

The types shown above can be interpreted as follows:

Type A — No threat/risk due to lack of any classified or controlled information.

a "non-existent"

Type B — No threat/risk; all persons with same clearance and access approvals.

Type C — Minimum threat/risk. All persons with same clearance, some with different or no approvals.

standards.

Type E — Maximum threat/risk different clearance standards and sensitive information co-resident and available.

One can map the various threat environments to the types of computer systems classes (from the DODCSC criteria) in a relatively straightforward way. The table below shows one cut at setting the security requirements for the various threat/risk environments taking into account, user functionality.

Threat/Risk Type	Minimum Security Class	Transaction Use Only
Type A	C1	C1
Type B	C1	C1
Type C	C2	C1
Type D	B2	B1
Type E	A2	A1/B3

Computer System Security Class
As a Function of Threat/Risk Type
and User Functionality